Bonner C. Walsh (OSB No. 131716)
bonner@walshpllc.com
WALSH LLC
1561 Long Haul Road
Grangeville, ID 83530
Tel: (541) 359-2827

Christopher D. Jennings (*pro hac vice* forthcoming)
chris@yourattorney.com
Nathan I. Reiter III (*pro hac vice* forthcoming)
nathan@yourattorney.com
THE JOHNSON FIRM
610 President Clinton Ave., Suite 300
Little Rock, AR 72201
Tel: (501) 372-1300

Brian C. Gudmundson (*pro hac vice* forthcoming)
brian.gudmundson@zimmreed.com
Jason P. Johnston (*pro hac vice* forthcoming)
jason.johnston@zimmreed.com
ZIMMERMAN REED
1100 IDS Center, 80 South 8th Street
Minneapolis, MN 55402
Tel: (612) 341-0400

Attorneys for Plaintiff and the Proposed Class

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF OREGON

PORTLAND DIVISION

LYNDA KINNE, individually and on behalf of all others similarly situated, *Plaintiff,* vs. AVAMERE HEALTH SERVICES, LLC, *Defendant*.	CIVIL ACTION NO. 3:22-cv-1400 CLASS ACTION COMPLAINT DEMAND FOR JURY TRIAL

CLASS ACTION COMPLAINT

Plaintiff, Lynda Kinne, ("Plaintiff"), individually and on behalf of all others similarly situated, brings this Class Action Complaint against Avamere Health Services, LLC, ("AHS" or "Defendant") and alleges upon personal knowledge as to her own actions and her counsels' investigations, and upon information and belief as to all other matters as follows:

NATURE OF THE ACTION

1. As a result of the lax security on AHS's network, Plaintiff and at least 197,000 other individuals have had the most sensitive details of their lives and identities accessed and stolen by malicious cybercriminals.

2. On an unknown date between March 17, 2022, and May 18, 2022, AHS learned that intermittent unauthorized access to its network occurred from January 19, 2022, to March 17, 2022. On information and belief, the unauthorized party removed files and folders from AHS's network (the "Data Breach").

3. As a result, Defendant lost control of highly sensitive files belonging to approximately 197,730 individuals.[1] The files contained personally identifiable information ("PII") and protected health information ("PHI") of Defendant's customers' current and former patients and employees including "identifiable protected health information such as full names, addresses, dates of birth, driver's license or state identification numbers, Social Security numbers, claims information, financial account numbers, medications information, lab results, and medical diagnosis/conditions information." (collectively, "Sensitive Information")

[1] Exhibit 1 ("Website Notice of Data Security Incident"), available at https://www.avamere.com/data-security-incident/#:~:text=On%207%2F13%2F22%2C,2022%20and%20March%2017%2C%202022. (last accessed Aug. 19, 2022).

4. Not only did Defendant fail to properly protect its customers' current and former patients' and employees' PII and PHI, Defendant failed to timely notify victims of the Data Breach.

5. On information and belief, Defendant began notifying victims about the Data Breach on July 13, 2022–over four months after discovering the breach and seven months after the breach began–Defendant has failed to explain why it took so long to notify breach victims.

6. When Defendant finally announced the Data Breach, it deliberately underplayed the Breach's severity and obfuscated the nature of the Breach. Defendant's notice sent to impacted individuals fails to explain how many people were impacted, how the breach happened, or why it took over four months to send a bare-bones notice to impacted individuals. In its "What Happened?" Section, the Notice provides one sentence devoid of any detail describing the Breach that occurred.

7. Plaintiff and members of the proposed Class are victims of Defendant's negligent and/or careless acts and omissions and the failure to protect PII and PHI of Plaintiff and members of the Class.

8. On information and belief, cybercriminals were able to breach Defendant's systems because Defendant did not maintain reasonable, up-to-date security practices and protocols to prevent the Data Breach that occurred. In fact, Defendant confirmed as much in its Breach Notice: "Since the incident, our Information Technology ("IT") department and external security experts have reviewed and enhanced our systems to reduce the chance of a similar event from occurring in the future."[2]

9. Prior to notification of the breach, Plaintiff and members of the proposed Class had no idea their PII and PHI had been compromised, and that they were, and continue to be, at

[2] Exhibit 2, Lynda Kinne Notice Letter

significant risk of identity theft and various other forms of personal, social, and financial harm. This risk will carry on for the duration of their lifetimes.

10. Defendant's failure to timely detect and notify breach victims violates Oregon law and has made Plaintiff and members of the Class (defined *infra*) vulnerable to a present and continuing risk of fraud and identity theft.

11. For example, armed with Sensitive Information acquired in the Data Breach, data thieves are able to commit numerous crimes including opening new financial accounts in members of the proposed Class's names, using members of the proposed Class's names to obtain government benefits, filing fraudulent tax returns, obtaining driver's licenses in members of the proposed Class's names but with another person's photograph, giving false information to police during an arrest, taking out loans in members of the proposed Class's names, and using members of the proposed Class's names to obtain medical services. Accordingly, Plaintiff and members of the proposed Class must now and for the foreseeable future closely monitor their financial and other accounts to guard against identity theft and related harm.

12. As a result of AHS's conduct, Plaintiff and the Class have and will be required to continue to undertake and incur out-of-pocket, expensive, and time-consuming efforts to mitigate the actual and potential impact of the Data Breach on their lives by, among other things, placing freezes and alerts with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, changing passwords on medical portals, and requesting and maintaining accurate medical records outside of those kept by medical providers.

13. Plaintiff brings this class action against Defendant for its failure to properly secure and safeguard the private and sensitive information it collected, maintained, stored, analyzed, and used in its ordinary course of business.

14. Plaintiff and the members of the proposed Class therefore bring this lawsuit seeking remedies including damages, reimbursement of out-of-pocket-costs, and equitable and injunctive relief, including improvements to Defendant's data security systems, future annual audits, and identity protection services funded by Defendant.

THE PARTIES

15. Plaintiff, Lynda Kinne, is a natural person and citizen of the State of Oregon, residing in Clackamas County, Oregon.

16. Defendant, Avamere Health Services, LLC ("AHS") is a domestic limited liability corporation, organized under the laws of Oregon, conducting business in Oregon, and with its headquarters and principal place of business at 25115 SW Parkway, Suite B, Wilsonville, Clackamas County, Oregon.

17. All of Plaintiff's claims stated herein are asserted against Defendant and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

JURISDICTION AND VENUE

18. This Court has subject matter jurisdiction and diversity jurisdiction over this action pursuant to 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds $5 million, exclusive of interest and costs, there are more than 100 members of the proposed class, and at least one Class Member is a citizen of a state different from Defendant to establish minimal diversity jurisdiction. AFC's operations span 300 locations across 20 states.

19. The District of Oregon has personal jurisdiction over Defendant because Defendant conducts substantial business in Oregon and in this District through its headquarters, offices, parents, and affiliates.

20. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b) because the Defendant and/or their parents or affiliates are headquartered and do business in this District and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District.

COMMON FACTUAL ALLEGATIONS

21. Plaintiff and members of the proposed Class are individuals who whose PII and/or PHI was accessed and/or exfiltrated during the Data Breach described in the Notice provided by Defendant.[3]

A. Background

22. Defendant, AHS, belongs to the Avamere Family of Companies ("AFC"). On their website, Avamere lists a few of the organizations that belong to AFC, including: Avamere Living; Infinity Rehab; Ovation by Avamere; Point Development Company; Signature CareConnect; Signature Healthcare at Home; and Therapy Solutions.[4] AFC is spread over 20 states, with 300 locations, and over 8,000 employees.[5] Avamere Health Services, LLC provides information technology services to healthcare providers, including its own affiliates and/or subsidiaries within AFC, such as Avamere Home Health Services, Mountain View Rehab, and Premere Rehab. [6]

[3] Ex. 1.
[4] https://www.avamere.com/press/the-avamere-family-of-companies-showcases-quality-care-in-annual-report/ (last accessed Aug. 29, 2022).
[5] https://www.avamere.com/our-story/ (last accessed Aug. 29, 2022).
[6] Ex. 2.

23. Defendant's customers require their patients and employees to provide them with some of their most sensitive and confidential information, including their PII and PHI. Defendant is then provided with this sensitive information in its ordinary course of business. Defendant maintains patients and/or employee full names, addresses, Social Security numbers, dates of birth, financial information, health insurance information, medical information, diagnosis, health insurance individual policy number, and Medicare/Medicaid information. This includes information that is static, does not change, and can be used to commit myriad financial crimes.

24. The Avamere Family of Companies, including Defendant, inform their patients and/or customers that they collect and maintain PII and PHI through AFC's Notice of Privacy Practices (the "Privacy Policy").[7]

25. The Privacy Policy states that Defendant is required "to implement policies and procedures to safeguard the privacy of your protected health information."[8]

26. Defendant had a duty to adopt reasonable measures to protect Plaintiff's and members of the proposed Class's PII and PHI from involuntary disclosure to third parties.

27. Upon information and belief, Defendant failed to properly implement, maintain, and safeguard their computer systems, networks, and data as well as to implement and maintain reasonable cybersecurity protocols, including, but not limited to:

a. Failing to maintain an adequate data security system to reduce the risks of data breaches and cyber attacks;

[7] Exhibit 3, ("AFC Joint Privacy Policy") available at: https://www.avamere.com/privacy-policy/ (last accessed Aug. 29, 2022).
[8] *Id.*

b. Failing to properly monitor its own data security systems for existing intrusion, brute force attempts, and clearing of logs;

c. Failing to apply all available security updates;

d. Failing to install the latest software patches, update its firewalls, check user account privileges; or ensure proper security practices;

e. Establishing effective password management and encryption protocols, including, but not limited to, the use of Multi-Factor Authentication for all users;

f. Locking, encrypting, and limiting access to computers and files containing sensitive information;

g. Implementing guidelines for maintaining and communicating sensitive data;

h. Protecting sensitive patient information, including personal and financial information, by implementing protocols on how to request and respond to requests for the transfer of such information and how to securely send such information through a secure file transfer system to only known recipients; and

i. Providing focused cybersecurity awareness training programs for employees.

28. Defendant's negligent conduct caused the Data Breach. Defendant violated its obligation to implement reasonable data security practices and to comply with industry standards.

B. The Data Breach and Notice Letter

29. On or around January 19, 2022, one or more intruders gained unauthorized access to Defendant's network.[9] Upon information and belief, malicious actors gained and maintained unfettered access to AHS's network, traveling through the AHS system in and out of areas where highly sensitive PII and PHI are kept. These malicious actors were undetected for three months, or until March 17, 2022, allowing them to copy and export substantial amounts of PII and PHI. Defendant said the intruder(s) had access to and potentially removed patient and employee files that contained identifiable protected health information such as full names, addresses, dates of birth, driver's license or state identification numbers, Social Security numbers, claims information, financial account numbers, medications information, lab results, and medical diagnosis/conditions information.[10] (the "Data Security Incident")

30. On or about July 13, 2022, Defendant ultimately admitted to the Data Breach. Defendant posted the Notice of the Breach on the Avamere website and sent out Notice letters to impacted individuals. On or about the same day, AHS reported the Breach to the United States Department of Health and Human Services' Office for Civil Rights ("DHHS").[11]

31. Given that Defendant was storing the PII and PHI of Plaintiff and the Class, Defendant was obligated to implement reasonable measures to prevent and detect cyber-attacks, such as those recommended by the Federal Trade Commission or other agencies and required by the Health Insurance Portability and Accountability Act. That obligation stems from the foreseeable risk of a Data Breach given that AHS collected, stored, and had access to a host of

[9] *See* Ex. 1.
[10] *Id.*
[11] U.S. DHHS OFFICE FOR CIVIL RIGHTS, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last accessed Aug. 19, 2022).

highly sensitive patient and employee records and data and, additionally, because of other highly publicized data breaches at different healthcare institutions and vendors.

32. The Data Breach itself, and information AHS has disclosed about the breach to date, indicate AHS failed to implement reasonable measures to prevent cyber-attacks and the exposure of Sensitive Information including its customers' patient and employee PHI and PII.

33. Despite the highly sensitive nature of the information AHS obtained, created, and stored, and the prevalence of data breaches of this nature, AHS inexplicably failed to take appropriate steps to safeguard the PII and PHI of Plaintiff and the Class from being compromised.

34. In the AFC joint privacy policy, Defendant promises, "You have the right to receive notice of an access, acquisition, use or disclosure of your health information that is not permitted by HIPAA, if such access, acquisition, use or disclosure compromises the security or privacy of your PHI (we refer to this as a breach). We will provide such notice to you without unreasonable delay but in no case later than 60 days after we discover the breach."

35. In direct contravention of the promise it made to Plaintiff and Class Members and in a willful and reckless manner, Defendant waited seven months after the Breach and nearly four months after discovering the Breach, before notifying impacted individuals that their Sensitive Information was in the hands of cyber criminals.

36. In the Notice, Defendant admitted that:

> We are writing to inform you of a data security incident involving some of your information in connection with services provided to you by Avamere Home Health Care, LLC, Mountain View Rehab, LLC, and Infinity Rehab.
>
> After an extensive forensic investigation, we concluded on May 18, 2022 that the files and folders that were potentially removed from our system contained identifiable protected health information such as full names, addresses, dates of birth, driver's license or state identification numbers, Social Security numbers, claims information, financial account numbers,

> medications information, lab results, and medical diagnosis/conditions information.

37. Defendant identified only the following actions it undertook to mitigate and remediate the harm caused by the Data Breach in the Notice Letter:

> Notified individuals have been provided complimentary credit monitoring services as well as best practices to protect their information, including but not limited to reviewing the explanation of benefits statements they receive from their health insurance providers and following up on any items or services not recognized.
>
> The security and privacy of personal information is of the utmost importance. Since the incident, our Information Technology ("IT") department and external security experts have reviewed and enhanced our systems to reduce the chance of a similar event from occurring in the future.

38. Defendant recognized the substantial and high likelihood that Plaintiff's and the proposed Class's PII would be misused following the Data Breach by, among other things, suggesting they engage in several time-consuming mitigation efforts as outlined in its Notice. [12]

39. Defendant should have prevented this Data Breach. Data Breaches are a well-known and publicized problem, thus putting Defendant on notice that the Sensitive Information in its possession was sought after and could be targeted by unauthorized parties or "hackers."

C. Healthcare Providers and Vendors Like Defendant are prime targets for Cybercriminals because of the Value of the Sensitive Information they Acquire, Collect, Maintain, and Use

40. Data breaches have become alarmingly commonplace in the U.S. In 2021, data breaches increased by nearly 70% over the previous year, which is over 20% higher than the previous all-time high.[13]

---

[12] *Id.*

[13] *2021 Annual Data Breach Year-End Review*, ITRC, (Jan. 2022), https://www.idtheftcenter.org/publication/2021-annual-data-breach-report-2/

41. Furthermore, the healthcare sector was the easiest "mark" among all major sectors last year, meaning it had the highest number of data compromises and categorically had some of the most widespread exposure per data breach.[14] According to the 2021 Healthcare Information and Management Systems Society Cybersecurity Survey, 67% of participating hospitals reported having a significant security incident within the last twelve months, with a majority of those being caused by "bad actors."[15]

42. Healthcare providers and vendors that maintain health care provider data "have emerged as a primary target because they sit on a gold mine of sensitive personally identifiable information for thousands of patients at any given time. From social security and insurance policies to next of kin and credit cards, no other organization, including credit bureaus, have so much monetizable information stored in their data centers.[16]

43. Cybercriminals recognize and exploit the value of PHI and PII. The value of PHI and PII is the foundation to the cyberhacker business model.

44. Likewise, the Federal Trade Commission ("FTC") has recognized that consumer data is a lucrative (and valuable) form of currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour underscored this point by reiterating that "most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency."[17]

---

[14] *Id.*

[15] *2021 HIMSS Cybersecurity Survey*, Healthcare Information and Management Systems Society, Inc., accessible at: https://www.himss.org/resources/himss-healthcare-cybersecurity-survey (last accessed Mar. 16, 2022).

[16] Benishti, Eyal, *How to Safeguard Hospital Data from Email Spoofing Attacks*, INSIDE DIGITAL HEALTH (Apr. 4, 2019), https://www.idigitalhealth.com/news/how-to-safeguard-hospitaldata-from-email-spoofing-attacks.

[17] Statement of FTC Commissioner Pamela Jones Harbour—Remarks Before FTC Exploring Privacy Roundtable, (Dec. 7, 2009) (last visited Jan. 18, 2022)

45. PII data for sale is so valuable because PII is so broad, and it can therefore be used for a wide variety of criminal activity such as creating fake IDs, buying medical equipment and drugs that can be resold on the street, or combining patient numbers with false provider numbers to file fake claims with insurers, opening new financial accounts, obtaining government benefits, filing fraudulent tax returns, giving false information to police during an arrest, taking out loans, and to obtain medical services.[18]

46. The static PII stolen in the Data Breach is significantly more valuable than the loss of non-static information, for example, credit card information in a large retailer data breach. Victims affected by those retailer breaches could avoid much of the potential future harm by simply cancelling credit or debit cards and obtaining replacements. The information compromised in the Data Breach—Social Security number, name, date of birth, etc.—is static and cannot reasonably be changed.

47. This data, as one would expect, demands a much higher price on the dark web. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[19] Likewise, the FBI has warned healthcare organizations that PII data is worth 10 times as much as personal credit card data on the black market.[20]

---

http://www/ftc/gov/speeches/harbour/091207privacyroundtable.pdf.

[18] *What to Know About Identity Theft,* FED TRADE COMM'N (April 2021), https://consumer.ftc.gov/articles/what-know-about-identity-theft

[19] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT WORLD (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hackpersonaldata-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html.

[20] Stolen PHI health credentials can sell for up to 20 times the value of a U.S. credit card number, according to Don Jackson, director of threat intelligence at PhishLabs, a cyber-crime protection company who obtained his data by monitoring underground exchanges where cyber-criminals sell the information. *See* Humer, Caroline & Finkle, Jim, *Your medical record is worth more to hackers than your credit card*, REUTERS, (Sep. 24, 2014),

48. Therefore, the value of Plaintiff's PII on the black market is considerable. Stolen PII trades on the black market for years, and criminals frequently post stolen private information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

49. As further evidence of the high value cybercriminals place on the Sensitive Information held by Defendant, one need look no further than the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, $1,250 is the reported average value on the dark web for an individuals' identity in the U.S.[21] Additionally, personal information can be sold at a price ranging from $40 to $200.[22] Medical records, however, can sell for up to $1,000 each, depending on how complete they are.[23] Alternatively, criminals are able to purchase access to entire company data breaches for $900 to $4,500.[24]

50. With over 1,000 data breaches per year over the past five years, Defendant was well aware the Sensitive Information it collects and uses is highly sensitive and of significant value to those who would use it for wrongful purposes.

---

https://www.reuters.com/article/uscybersecurity-hospitals/your-medical-record-is-worth-more-to-hackers-than-your-credit-cardidUSKCN0HJ21I20140924. Dark web monitoring is a commercially available service which, at a minimum, AHS can and should perform (or hire a third-party expert to perform).

[21] *Dark Web Market Prices: How Much Is Your Data Worth*?, Top10VPN, https://www.top10vpn.com/research/dark-web-prices/ (last accessed Mar. 16, 2022)

[22] *Your Personal Data Is For Sale on the Dark Web. Here's How Much It Costs*, DIGITAL TRENDS (Oct. 16, 2019), https://digitaltrends.com/cpmputing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed Mar. 16, 2022).

[23] *What is Your Personal Information Worth on the Dark Web*, HIPAA SECURE NOW!, (Feb. 8, 2018), https://www.hipaasecurenow.com/what-is-your-personal-information-worth-on-the-dark-web/ (last accessed Mar. 16, 2022).

[24] *In the Dark*, VPNOVERVIEW (2019), https://www.vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed Mar. 16, 2022)

51. Because the Sensitive Information exposed in the AHS Data Breach is permanent data, there may be a gap of time between when it was stolen and when it will be used. The damage may continue for years. Plaintiff and the Class now face years of monitoring their financial and personal records with a high degree of scrutiny. The Class has incurred and will incur this damage in additional to any fraudulent use of their Sensitive Information.

D. Defendant failed to sufficiently protect the PII and PHI entrusted to it

(i). Defendant failed to adhere to HIPAA

52. HIPAA circumscribes security provisions and data privacy responsibilities designed to keep medical information safe. HIPAA compliance provisions, commonly known as the Administrative Simplification Rules, establish national standards for electronic transactions and code sets to maintain the privacy and security of protected health information.[25]

53. HIPAA provides specific privacy rules that require comprehensive administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of PII is properly maintained.[26]

54. Defendant's Data Breach resulted from a combination of inadequacies showing it failed to comply with safeguards mandated by HIPAA. Defendant's security failures include, but are not limited to:

[25] HIPAA lists eighteen types of information that qualify as PHI according to guidance from the Department of Health and Human Services Office for Civil Rights, and includes, inter alia: names, addresses, any dates including dates of birth, social security numbers, and medical record numbers.
[26] *See* 45 C.F.R. § 164.306 (Security standards and General rules); 45 C.F.R. § 164.308 (Administrative safeguards); 45 C.F.R. § 164.310 (Physical safeguards); 45 C.F.R. § 164.312 (Technical safeguards).

a. Failing to ensure the confidentiality and integrity of electronic PII that it creates, receives, maintains, and transmits, in violation of 45 C.F.R. § 164.306(a)(1);

b. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PII, in violation of 45 C.F.R. § 164.306(a)(2);

c. Failing to protect against any reasonably anticipated uses or disclosures of electronic PII that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 C.F.R. § 164.306(a)(3);

d. Failing to ensure compliance with HIPAA security standards by Defendant's workforce, in violation of 45 C.F.R. § 164.306(a)(4);

e. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PII to allow access only to those persons or software programs that have been granted access rights, in violation of 45 C.F.R. §164.312(a)(1);

f. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 C.F.R. § 164.308(a)(1);

g. Failing to identify and respond to suspected or known security incidents and failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity, in violation of 45 C.F.R. § 164.308(a)(6)(ii);

h. Failing to effectively train all staff members on the policies and procedures with respect to PII as necessary and appropriate for staff members to carry out their functions and to maintain security of PII, in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5); and

i. Failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PII, in compliance with 45 C.F.R. § 164.530(c).

(ii). Defendant failed to adhere to FTC guidelines

55. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making.[27] To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as AHS, should employ to protect against the unlawful exposure of PII.

56. In 2016, the FTC updated its publication Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business.[28] The guidelines explain that businesses should:

a. Protect the personal customer information that they keep;

b. Properly dispose of personal information that is no longer needed;

c. Encrypt information stored on computer networks;

d. Understand their network's vulnerabilities; and

e. Implement policies to correct security problems.

[27] *Start with Security: A Guide for Business*, FED. TRADE COMM'N (Sep. 2, 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.
[28] *Protecting Personal Information: A Guide for Business*, FED. TRADE COMM'N (Sep. 28, 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting personalinformation.pdf.

57. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

58. The FTC recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[29]

59. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

60. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to patient PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

(iii). Defendant failed to adhere to industry standards

61. As stated above, the healthcare industry continues to be a high value target among cybercriminals. In 2021, the U.S. healthcare sector experienced over 330 data breaches, a number which is likely to continue to grow.[30] The costs of healthcare data breaches per record are among

[29] *See Start with Security*, *supra* note 28.
[30] *2021 Annual Data Breach Year-End Review*, ITRC, (Jan. 2022), https://www.idtheftcenter.org/publication/2021-annual-data-breach-report-2/

the highest across all industries and are well over the global average per record.[31] As a result, both the government and private sector have developed industry best standards to address this growing problem.

62. The United States Department of Health and Human Services' Office for Civil Rights ("DHHS") notes that, "[w]hile all organizations need to implement policies, procedures, and technical solutions to make it harder for hackers to gain access to their systems and data, this is especially important in the healthcare industry. Hackers are actively targeting healthcare organizations as they store large quantities of highly sensitive and valuable data."[32] DHHS highlights "several basic cybersecurity safeguards that can be implemented to improve cyber resilience which only require a relatively small financial investment, yet they can have a major impact on an organization's cybersecurity posture."[33] Most notably, organizations must properly encrypt PII to mitigate against misuse.

63. The private sector has similarly identified the healthcare sector as particularly vulnerable to cyberattacks both because of the of value of the PII that it maintains and because, as an industry, it has been slow to adapt and respond to cybersecurity threats.[34]

64. Despite the abundance and availability of information regarding cybersecurity best practices for the healthcare industry, Defendant failed to adopt sufficient data security processes, a fact highlighted in its notification to affected patients in which it revealed that only after the Data Breach, Defendant has taken steps to increase the security of its systems. Defendant stated, "The

---

[31] *Id.*
[32] *Cybersecurity Best Practices for Healthcare Organizations*, HIPAA JOURNAL (Nov. 1, 2018), https://www.hipaajournal.com/important-cybersecurity-best-practices-for-healthcare-organizations/ (last accessed Mar. 16, 2022).
[33] *Id.*
[34] *10 Cyber Security Best Practices For the Healthcare Industry*, NTIVA (Jun. 19, 2018), https://www.ntiva.com/blog/10-cybersecurity-best-practices-for-the-healthcare-industry.

security and privacy of personal information is of the utmost importance. Since the incident, our Information Technology ("IT") department and external security experts have reviewed and enhanced our systems to reduce the chance of a similar event from occurring in the future."[35] The Data Breach at issue here was the inevitable result of Defendant's inadequate approach and/or attention to data security protection of the Sensitive Information it collects, analyzes, and uses in its ordinary course of business.

65. Moreover, Defendant failed to properly implement, maintain, and safeguard its computer systems, networks, and data including (but not limited to):

a. Failing to maintain an adequate data security system to reduce the risks of data breaches and cyber attacks;

b. Failing to properly monitor its own data security systems for existing intrusion, brute force attempts, and clearing of logs;

c. Failing to apply all available security updates; and

d. Failing to install the latest software patches, updates its firewalls, check user account privileges; or ensure proper security practices.

66. Defendant's failure to implement these rudimentary measures made it an easy target for the Data Breach.

E. Plaintiff and the Class Members were significantly harmed by the Data Breach

67. The personal, health, and financial information of Plaintiff and the Class, is valuable and has become a highly desirable commodity to data thieves.

68. Defendant's failure to reasonably safeguard Plaintiff's and the Class's sensitive PHI and PII has created a serious risk to Plaintiff and the Class, including both a short-term and

[35] Ex. 1.

long-term risk of identity theft.

69. Identity theft occurs when someone uses another's personal and financial information such as that person's name, account number, Social Security number, driver's license number, date of birth, and/or other information, without permission, to commit fraud or other crimes.

70. According to experts, one out of four data breach notification recipients become a victim of identity fraud.[36]

71. Stolen Sensitive Information is often trafficked on the "dark web," a heavily encrypted part of the Internet that is not accessible via traditional search engines that is frequented by criminals, fraudsters, and other wrongdoers. Law enforcement has difficulty policing the "dark web," which allows users and criminals to conceal their identities and online activity.

72. Purchasers of Sensitive Information use it to gain access to the victim's bank accounts, social media, credit cards, and tax details. This can result in the discovery and release of additional Sensitive Information from the victim, as well as Sensitive Information from family, friends, and colleagues of the original victim. Victims of identity theft can also suffer emotional distress, blackmail, or other forms of harassment in person or online. Losses encompass financial data and, tangible money, along with unreported emotional harms.

73. The FBI's Internet Crime Complaint (IC3) 2019 estimated there was more than $3.5 billion in losses to individual and business victims due to identity fraud in that year alone. The same report identified "rapid reporting" as a tool to help stop fraudulent transactions and mitigate losses.

[36] *Study Shows One in Four Who Receive Data Breach Letter Become Fraud Victims*, ThreatPost.com (last visited Jan. 17, 2022), https://threatpost.com/study-shows-one-four-whoreceive-data-breach-letter-become-fraud-victims-022013/77549/

74. AHS did not rapidly, or even reasonably, report to Plaintiff and the Class that their Sensitive Information had been stolen. In addition, the fact that the PII and PHI obtained in the Breach involved sensitive medical information exacerbated the harm to Plaintiff and the Class.

75. As discussed above, PII and PHI are among the most sensitive and personally damaging information. A report focusing on breaches in the healthcare industry found that the "average total cost to resolve an identity theft-related incident . . . came to about $20,000.00" per person, and that the victims were further routinely forced to pay out-of-pocket costs for health care they did not receive in order to restore coverage.[37]

76. Victims of medical identity theft can suffer significant financial consequences. "In some cases, they must pay the healthcare provider, repay the insurer for services obtained by the thief, or . . . engage an identity service provider or legal counsel to help resolve the incident and prevent future fraud."[38]

77. Moreover, nearly half of identity theft victims lost their health care coverage as a result of a data breach incident, nearly one-third reported that their premiums went up, and forty percent never resolved their identity theft at all.[39]

78. "Unfortunately, by the time medical identity theft is discovered, the damage has been done. Forty percent of consumers say that they found out they were a victim of medical identity theft only when they received collection letters from creditors for expenses that thieves

[37] Elinor Mills, Study: *Medical identity theft is costly for victims*, CNET (Mar. 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/.
[38] *Fifth Annual Study on Medical Identity Theft*, PONEMON INSTITUTE LLC 1 (Nov. 18, 2015), https://static.nationwide.com/static/2014_Medical_ID_Theft_Study.pdf?r=65.
[39] *Id.*

incurred in their name. As a result, the consequences of medical identity theft are frequently severe, stressful, and expensive to resolve."[40]

79. Moreover, resolution of medical identity theft is time consuming to remedy. "Due to HIPAA privacy regulations, victims of medical identity theft must be involved in the resolution of the crime. In many cases, victims struggle to reach resolution following a medical identity theft incident."[41] Consequently, they remain at "risk for further theft or errors in their healthcare records that could jeopardize medical treatments and diagnosis."[42]

80. These consequences are further exacerbated when, like here, the PII compromised includes Social Security numbers, which make it possible for cybercriminals to perpetrate the most serious types of fraud such as filing tax returns, seeking unemployment benefits, or even applying for a job using a false identity. Each of these fraudulent activities is difficult to detect and may not be uncovered until the number has already been used in a fraudulent transaction. Moreover, it is no easy task to cancel a stolen Social Security number, and even then "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[43]

---

[40] *The Potential Damages and Consequences of Medical Identity Theft and Healthcare Data Breaches*, EXPERIAN (Apr. 13, 2010), https://www.experian.com/assets/databreach/whitepapers/consequences-medical-id-theft-healthcare.pdf.

[41] *Id.*

[42] *Id.*

[43] Naylor, B., *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-hasmillions-worrying-about-identity-theft.

81. The Social Security Administration has warned that identity thieves can use stolen Social Security numbers to apply for additional credit lines. Such fraud may go undetected until debt collection calls commence months, or even years, later.[44]

82. As a result of the Data Breach, Plaintiff and Class Members now face, and will continue to face, a heightened risk of identity theft and fraud for the rest of their lives.

83. As a long-standing member of the health care community through its role as an information technology vendor to healthcare providers, Defendant knew or should have known the importance of safeguarding patient and employee PII and PHI entrusted to it and of the foreseeable consequences of a breach. Despite this knowledge, however, Defendant failed to take adequate cyber-security measures to prevent this Data Breach from occurring.

84. Defendant has not provided any compensation to patients or employees victimized in the Data Breach. Defendant merely offered a 12-month subscription to IDX identity protections services.

85. Even if Defendant did reimburse Plaintiff and Class Members for the harm they suffered, it is incorrect to assume that reimbursing a victim of the Data Breach for financial loss due to fraud makes that individual whole again. On the contrary, after conducting a study, the U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems" and that "resolving the problems caused by identity theft [could] take more than a year for some victims."[45]

---

[44] *Identity Theft and Your Social Security Number*, SOCIAL SECURITY ADMIN. (June 2018), http://www.ssa.gov/pubs/EN-05-10064.pdf.

[45] *Victims of Identity Theft*, 2012, U.S. DEP'T OF JUSTICE 10, 11 (Jan. 27, 2014), https://www.bjs.gov/content/pub/pdf/vit12.pdf.

86. As a result of Defendant's failure to prevent the Data Breach, Plaintiff and Class Members have suffered and will continue to suffer significant damages. They have suffered or are at increased risk of suffering:

a. The loss of the opportunity to control how their PII and PHI is used;

b. The diminution in value of their PII;

c. The compromise, publication, and/or theft of their PII and PHI;

d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud, including the purchase of identity theft protection insurance and detection services;

e. Lost opportunity costs and lost wages associated with the time and effort expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Disclosure, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen PII and PHI;

h. The continued risk to their PII and PHI, which remains in the possession of Defendant and is subject to further breaches so long as Defendant fails to undertake appropriate measures to protect the PII and PHI in their possession;

i. Current and future costs related to the time, effort, and money

that will be expended to prevent, detect, contest, remediate, and repair the impact of the Data Breach for the remainder of the lives of Plaintiff and Class Members; and

j. Stress, anxiety, and other related forms of emotional distress.

87. In addition to remedy for these harms, Plaintiff and members of the proposed Class maintain an undeniable interest in ensuring their Sensitive Information is secure, remains secure, and is not subject to further misappropriation and/or theft.

F. Defendant's Delay in Identifying and Reporting the Breach Caused Additional Harm

88. It is axiomatic that:

> The quicker a financial institution, credit card issuer, wireless carrier or other service provider is notified that fraud has occurred on an account, the sooner these organizations can act to limit the damage. Early notification can also help limit the liability of a victim in some cases, as well as allow more time for law enforcement to catch the fraudsters in the act.[46]

89. Indeed, once a data breach has occurred:

> [o]ne thing that does matter is hearing about a data breach quickly. That alerts consumers to keep a tight watch on credit card bills, insurance invoices, and suspicious emails. It can prompt them to change passwords and freeze credit reports. And notifying officials can help them to catch cybercriminals and warn other businesses of emerging dangers. If consumers don't know about a breach because it wasn't reported, they can't take action to protect themselves (internal citations omitted). [47]

---

[46] *Identity Fraud Hits Record High with 15.4 Million U.S. Victims in 2016, Up 16 Percent According to New Javelin Strategy & Research Study,* BUSINESS WIRE, https://www.businesswire.com/news/home/20170201005166/en/Identity-Fraud-Hits-Record-High-15.4-Million (last accessed Mar. 21, 2022).

[47] *The Data Breach Next Door Security breaches don't just hit giants like Equifax and Marriott. Breaches at small companies put consumers at risk, too,* CONSUMER REPORTS (January 31, 2019), https://www.consumerreports.org/data-theft/the-data-breach-next-door/ (last accessed Mar. 21, 2022).

90. Additionally, pursuant to 45 CFR § 164.404, and as outlined in the AFC Joint Privacy Policy, Defendant was required to provide notice to Plaintiff and members of the proposed class no later than 60 days after discovering the breach.

91. Although their Sensitive Information was improperly exposed, viewed, exfiltrated and/or stolen on or about January 19, 2022, affected persons were not notified of the Data Breach by Defendant until, at the earliest, July 13, 2022, depriving them of the ability to promptly mitigate potential adverse consequences resulting from the Data Breach.

92. As a result of Defendant's delay in detecting and notifying Plaintiff and members of the proposed Class of the Data Breach, Plaintiff's and members of the proposed Class's risk of fraud has been driven even higher.

PLAINTIFF'S EXPERIENCES

93. Lynda Kinne is a resident and citizen of Oregon. She is a former patient of a customer of Defendant.

94. Defendant acquired, collected, and stored, the PII and PHI of Ms. Kinne.

95. On or about mid-July of 2022, Lynda Kinne received notice from Defendant, which informed her of the Data Breach and that she faced a substantial and significant risk of her PII and PHI being misused.[48]

96. Subsequent to and as a direct and proximate result of the Data Breach, Ms. Kinne was the victim of identity theft when her personal information was used by an unknown individual who attempted to open a Capital One credit card in her name in July 2022 and then again in August

[48] Ex. 2.

2022.[49] In addition, following the Data Breach, she experienced a substantial number of spam emails, text messages, and phone calls, which Plaintiff believes is related to her private information being placed in the hands of an illicit actor. As a result, Ms. Kinne had to spend considerable time and efforts to mitigate against the attempted fraud and against any future identity theft and fraud. This included, but was not limited to, replacing all eight of her credit cards,

97. Plaintiff Kinne is very careful about sharing her sensitive PII and PHI. She has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source. Furthermore, Plaintiff Kinne stores any documents containing her sensitive information in a safe and secure location or destroys the documents. Moreover, she diligently chooses unique usernames and passwords for her various online accounts. Finally, Plaintiff Kinne has never previously had her identity stolen.

98. Plaintiff Kinne suffered actual injury from having her sensitive information exposed and/or stolen as a result of the Data Breach including, but not limited to: (a) injury arising from actual fraud and attempted theft; (b) damages to and diminution in the value of her Sensitive Information–a form of intangible property; (c) loss of her privacy; (d) continuous imminent and impending injury arising from the increased risk of financial, medical, and identity fraud and theft; and (e) time and expense of her mitigation efforts as a result of the data breach and subsequent fraud.

99. In addition, knowing that hackers accessed and/or stole her PII and PHI and that this information was used to commit fraud, and will likely continue to be used in the future for such purposes has caused Ms. Kinne to experience feelings of rage, anger, anxiety, sleep

[49] The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority. 17 C.F.R. § 248.201 (2013).

disruption, stress, fear, and physical pain. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that is contemplated and addressed by law.

CLASS ALLEGATIONS

100. Pursuant to Pursuant to Federal Rules of Civil Procedure 23(b)(2), 23(b)(3), and 23(c)(4), Plaintiff brings this action on behalf of herself and on behalf of all members of the proposed Classes (collectively, the "Class," "Classes," and "Class Members:) defined as:

> **Nationwide Class:** All individuals residing in the United States whose PII and/or PHI was stored or possessed by AHS that was actually or potentially compromised during the Data Breach as referenced in the Notice of Data Privacy Incident provided by Defendant.[50]
>
> **Oregon Subclass**: All residents of the State of Oregon whose PII and/or PHI was stored or possessed by AHS that was actually or potentially compromised during the Data Breach as referenced in the Notice of Data Privacy Incident provided by Defendant.[51]

101. The following people are excluded from the Classes: (1) any judge or magistrate presiding over this action and members of their families; (2) Defendant, Defendant's subsidiaries, parents, successors, predecessors, affiliated entities, and any entity in which Defendant or its parents have a controlling interest, and their current or former officers and directors; (3) persons who properly execute and file a timely request for exclusion from the Class; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiff's counsel and Defendant's counsel; and (6) the legal representatives, successors, and assigns of any such excluded persons.

[50] Ex. 1.
[51] *Id.*

102. Plaintiff and members of the Classes satisfy the numerosity, commonality, typicality, adequacy, and predominance prerequisites for suing as representative parties pursuant to Federal Rule of Civil Procedure 23.

103. **Numerosity, Fed. R. Civ. P. 23(a)(1):** The exact number of members of the Classes are unknown but, upon information and belief, they are estimated to number in the tens or hundreds of thousands at this time, and individual joinder in this case is impracticable. Members of the Classes can be easily identified through Defendant's records and objective criteria permitting self-identification in response to notice, and notice can be provided through techniques similar to those customarily used in other data breach, consumer breach of contract, unlawful trade practices, and class action controversies.

104. **Typicality, Fed. R. Civ. P. 23(a)(3)**: Plaintiff's claims are typical of the claims of other members of the Classes in that Plaintiff, and the members of the Classes sustained damages arising out of Defendant's Data Breach, wrongful conduct and misrepresentations, false statements, concealment, and unlawful practices, and Plaintiff and members of the Classes sustained similar injuries and damages, as a result of Defendant's uniform illegal conduct.

105. **Adequacy, Fed. R. Civ. P. 23(a)(4)**: Plaintiff will fairly and adequately represent and protect the interests of the Classes and has retained counsel competent and experienced in complex class actions to vigorously prosecute this action on behalf of the Classes. Plaintiff has no interests that conflict with, or are antagonistic to those of, the Classes, and Defendant has no defenses unique to Plaintiff.

106. **Commonality and Predominance, Fed. R. Civ. P. 23(a)(2) and (b)(3)**: There are many questions of law and fact common to the claims of Plaintiff and the Classes, and those

questions predominate over any questions that may affect individual members of the Classes. Common questions for the Classes include, but are not necessarily limited to the following:

a. Whether Defendant violated the laws asserted herein;

b. Whether Defendant had a duty to use reasonable care to safeguard Plaintiff's and members of the Classes' PII and PHI;

c. Whether Defendant breached the duty to use reasonable care to safeguard members of the Classes' PII and PHI;

d. Whether Defendant knew or should have known about the inadequacies of their data security policies and system and the dangers associated with storing sensitive PII and PHI;

e. Whether Defendant failed to use reasonable care and commercially reasonable methods to safeguard and protect Plaintiff's and members of the Classes' PII and PHI from unauthorized release and disclosure;

f. Whether the proper data security measures, policies, procedures, and protocols were in place and operational within Defendant's computer systems to safeguard and protect Plaintiff's and members of the Classes' PII and PHI from unauthorized release and disclosure;

g. Whether Defendant took reasonable measures to determine the extent of the Data Breach after it was discovered;

h. Whether Defendant's delay in informing Plaintiff and members of the Classes of the Data Breach was unreasonable;

i. Whether Defendant's method of informing Plaintiff and other members of the Classes of the Data Breach was unreasonable;

j. Whether Defendant is liable for negligence or gross negligence;

k. Whether Defendant's conduct, practices, statements, and representations about the Data Breach of the PII and PHI violated applicable state laws;

l. Whether Plaintiff and members of the Classes were injured as a proximate cause or result of the Data Breach;

m. What the proper measure of damages is; and

n. Whether Plaintiff and members of the Class are entitled to restitutionary, injunctive, declaratory, or other relief.

107. **Superiority, Fed. R. Civ. P. 23(b)(3):** This cause is also appropriate for class certification because class proceedings are superior to all other available methods for the fair and efficient adjudication of this controversy as joinder of all parties is impracticable. The damages suffered by the individual members of the Classes will likely be relatively small, especially given the burden and expense of individual prosecution of the complex litigation necessitated by Defendant's actions. Thus, it would be virtually impossible for the individual members of the Classes to obtain effective relief from Defendant's misconduct. Even if members of the Classes could sustain such individual litigation, it would still not be preferable to a class action, because individual litigation would increase the delay and expense to all parties due to the complex legal and factual controversies presented in this Complaint. By contrast, a class action presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court. Economies of time, effort, and expense will be fostered, and uniformity of decisions ensured.

108. A class action is therefore superior to induvial litigation because:

a. The amount of damages available to an individual Plaintiff is insufficient to make litigation addressing Defendant's conduct economically feasible in the absence of the class action procedural device;

b. Individualized litigation would present a potential for inconsistent or contradictory judgments, and increases the delay and expense to all parties and the court system; and

c. The class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

CAUSES OF ACTION

Count I
Negligence
(On Behalf of Plaintiff and the Nationwide Class)

109. Plaintiff and members of the Class incorporate the above allegations as if fully set forth herein.

110. AHS had duty to exercise reasonable care in safeguarding, securing, and protecting the Sensitive Information of Plaintiff and members of the Class from being compromised, lost, stolen, misused, and/or disclosed to unauthorized third parties. This duty includes, among other things, designing, maintaining, and testing AHS's security protocols to ensure that the PHI and PII of Plaintiff and members of the Class in AHS's possession was adequately secured and protected.

111. AHS also had a duty to exercise appropriate clearinghouse practices to remove PII and PHI it was no longer required to retain pursuant to regulations, including that of AHS's customers' current and former employees or patients.

112. AHS also had a duty to have procedures in place to detect and prevent the improper access and misuse of the PII and PHI of Plaintiff and members of the Class.

113. AHS's duty to use reasonable security measures arose because it was foreseeable that AHS's failure to adequately safeguard PII and PHI in accordance with industry standards concerning data security would result in the compromise of that PII and PHI—just like the Data Breach that ultimately came to pass. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiff's and members of the Class's PII and PHI by disclosing and providing access to this information to third parties and by failing to properly supervise both the manner in which the PHI was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

114. A breach of security, unauthorized access, and resulting injury to Plaintiff and members of the Class was reasonably foreseeable, particularly in light of AHS's inadequate security practices.

115. Plaintiff and members of the Class were the foreseeable and probable victims of any inadequate security practices and procedures. AHS knew or should have known of the inherent risks in collecting and storing the PII and PHI of Plaintiff and members of the Class, the critical importance of providing adequate security of that PII and PHI, and the necessity for encrypting PII and PHI stored on AHS's systems.

116. AHS's own conduct created a foreseeable risk of harm to Plaintiff and members of the Class. AHS's misconduct included, but was not limited to, its failure to take steps and opportunities to prevent the Data Breach as set forth herein. AHS's misconduct also included its decision not to comply with industry standards for the safekeeping of the PII and PHI of Plaintiff

and members of the Class, including basic encryption of the PII and PHI of Plaintiff and members of the Class, including basic encryption techniques freely available to AHS.

117. Plaintiff and Members of the Class had no ability to protect their PII and PHI that was in, and possibly remains in, AHS's possession.

118. AHS was in a position to protect against the harm suffered by Plaintiff and members of the Class as a result of the Data Breach.

119. AHS had and continues to have a duty to adequately and timely disclose that the PII and PHI of Plaintiff and members of the Class within AHS's possession might have been compromised, how it was compromised, and precisely the types of data compromised and when. Such notice was necessary to allow Plaintiff and members of the Class to take steps to prevent, mitigate, and repair identity theft and the fraudulent use of their PII and PHI by third parties.

120. AHS had a duty to employ proper procedures to prevent the unauthorized dissemination of the PII and PHI of Plaintiff and members of the Class.

121. AHS has admitted that the PII and PHI of Plaintiff and members of the Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

122. AHS, through its actions and/or omissions, unlawfully breached its duties to Plaintiff and members of the Class by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the PII and PHI of Plaintiff and members of the Class during the time the PII and PHI was within AHS's possession.

123. AHS improperly and inadequately safeguarded the PII and PHI of Plaintiff and members of the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

124. AHS failed to heed industry warnings and alerts to provide adequate safeguards to protect the PII and PHI of Plaintiff and members of the Class in the face of increased risk of theft.

125. AHS, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and members of the Class by failing to have appropriate procedures in place to detect and prevent dissemination of their PII and PHI.

126. AHS breached its duty to exercise appropriate clearinghouse practices by failing to remove PII and PHI it was no longer required to retain pursuant to regulations.

127. AHS, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiff and members of the Class the existence and scope of the Data Breach.

128. But for AHS's wrongful and negligent breach of its duties owed to Plaintiff and members of the Class, the PII and PHI of Plaintiff and members of the Class would not have actually or potentially been compromised.

129. There is a close causal connection between AHS's failure to implement security measures to protect the PII and PHI of Plaintiff and members of the Class and the harm, or risk of imminent harm suffered by Plaintiff and members of the Class. The PII and PHI of Plaintiff and the members of the Class was actually or potentially compromised as the proximate result of AHS's failure to exercise reasonable care in safeguarding such PII and PHI by adopting, implementing, and maintaining appropriate security measures.

130. As a direct and proximate cause of AHS's negligence Plaintiff and members of the Class have suffered or will suffer damages, including monetary damages, increased risk of future harm, loss of privacy, loss of value of PII and PHI, loss of time and resources to mitigate against

increased risk of future harm, embarrassment, humiliation, frustration, emotional distress, and other damages.

131. AHS's breach of its common law duties actually and proximately caused Plaintiff's and members of the Class's actual, tangible, injury-in-fact and damages.

132. Plaintiff and class members have suffered or are at an increased risk of suffering the theft of their PII and PHI by criminals; loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; lost control over the value of PII; unreimbursed losses relating to fraudulent charges; losses relating to exceeding credit and debit card limits and balances; harm resulting from damaged credit scores and information; emotional anguish; identity theft and fraud, and other harm resulting from the unauthorized use or threat of unauthorized use of stolen personal information, including personal health information, that resulted from and was caused by AHS's negligence, entitling them to damages in an amount to be proven at trial. Furthermore, injury-in-fact and damages are ongoing, imminent, immediate, and continue to be faced.

133. But for AHS's wrongful and negligent breach of its duties owed to Plaintiff and the Class, Plaintiff and the members of the Class would not have been injured.

134. The injury and harm suffered by Plaintiff and the members of the Class were the reasonably foreseeable result of AHS's breach of its duties. AHS knew or should have known that AHS was failing to meet its duties and that its breach would cause Plaintiff and members of the Class to suffer the foreseeable harms associated with the exposure of their PII and PHI.

135. As a direct and proximate result of AHS's negligence, Plaintiff and members of the Class are entitled to and demand actual, consequential, and nominal damages.

Count II
Negligence *Per se*
(On Behalf of Plaintiff and the Nationwide Class)

136. Plaintiff and members of the Class incorporate the above allegations as if fully set forth herein.

137. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as AHS, of failing to use reasonable measures to protect customers or, in this case, patients' PII and PHI. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of AHS's duty to protect Plaintiff's and members of the Class's sensitive PII and PHI.

138. AHS violated Section 5 of the FTC Act by failing to use reasonable measures to protect their customers' patients' and employees' PII and PHI. AHS's conduct was particularly unreasonable given the nature and amount of PII and PHI AHS had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to its customers' patients and employees in the event of a breach, which ultimately came to pass.

139. AHS's violation of Section 5 of the FTC Act constitutes negligence *per se*.

140. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, as a result of their failure to employ reasonable data security measures, caused the same harm as that suffered by Plaintiff and members of the Class.

141. AHS's violations of HIPAA also independently constitutes negligence *per se*.

142. HIPAA privacy laws were enacted with the objective of protecting the confidentiality of patients' healthcare information and set forth the conditions under which

information can be used, and to whom it can be disclosed. HIPAA privacy laws not only apply to healthcare providers and the organizations they work for, but to any entity that may have access to healthcare information about a patient that–if it were to fall into the wrong hands–could present a risk of harm to the patient's finances or reputation.

143. Plaintiff and members of the Class are within the class of persons HIPAA privacy laws were intended to protect.

144. The harm that occurred as a result of the Data Breach is the type of harm HIPAA privacy laws were intended to guard against.

145. As a direct and proximate cause of AHS's negligence *per se*, Plaintiff and members of the Class have suffered or will suffer damages, including monetary damages, identity theft, increased risk of future harm, loss of privacy, loss of value of PII and PHI, loss of time and resources to mitigate against increased risk of future harm, embarrassment, humiliation, frustration, emotional distress, and other damages.

146. AHS's breach of its statutory duties actually and proximately caused Plaintiff's and members of the Class's actual, tangible, injury-in-fact and damages.

147. Plaintiff and class members have suffered or are at an increased risk of suffering the theft of their PII and PHI by criminals; loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; lost control over the value of PII; unreimbursed losses relating to fraudulent charges; losses relating to exceeding credit and debit card limits and balances; harm resulting from damaged credit scores and information; emotional anguish; identity theft and fraud, and other harm resulting from the unauthorized use or threat of unauthorized use of stolen personal information, including personal health information, that resulted from and was caused by AHS's negligence *per se*, entitling them to damages in an

amount to be proven at trial. Furthermore, injury-in-fact and damages are ongoing, imminent, immediate, and continue to be faced.

148. But for AHS's wrongful and negligent breach of their statutory duties owed to Plaintiff and the Class, Plaintiff and the members of the Class would not have been injured.

149. The injury and harm suffered by Plaintiff and the members of the Class were the reasonably foreseeable result of AHS's breach of its duties. AHS knew or should have known that AHS was failing to meet its duties and that its breach would cause Plaintiff and members of the Class to suffer the foreseeable harms associated with the exposure of their PII and PHI.

150. As a direct and proximate result of Defendant's negligence *per se* Plaintiff and members of the Class are entitled to and demand actual, consequential, and nominal damages.

COUNT III
Violation of the Oregon Consumer Information Protection Act
ORS 646A.604
(On behalf of Plaintiff and the Oregon Subclass)

151. Plaintiff and members of the Oregon Subclass incorporate the above allegations as if fully set forth herein.

152. AHS is subject to the Oregon Consumer Information Protection Act ("CIPA"), which states: "A covered entity ... shall develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of personal information." ORS § 646A.622(1).

153. CIPA defines "covered entity" as a "person that owns, licenses, maintains, stores, manages, collects, processes, acquires or otherwise possesses personal information in the course of the person's business." ORS § 646A.602(5)(a). Defendant meets the definition of a covered entity as an Oregon limited liability corporation providing technology and data services to health care providers, including the storage of personal information.

154. The PII stolen in the Data Breach includes personal information that meets CIPA's definition under ORS § 646A.602.

155. As alleged throughout the complaint, AHS failed to maintain reasonable safeguards to protect Plaintiff and the Class's PII, thus violating CIPA.

156. Following the Data Breach, AHS further failed to undertake reasonable measures to timely determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of PII before notifying Plaintiffs and the Class of the Data Breach.

157. ORS 646A.604 requires an entity that is subject to a breach or receives notice of a breach of security to give notice of the breach to "the consumer to whom the personal information pertains." It further requires the breached entity to give notice of the security breach in "the most expeditious manner possible, without unreasonable delay, but not later than 45 days after discovering or receiving notification of the breach." *Id.* A violation of ORS 646A.600 to 646A.628 is an unlawful practice under ORS 646.607.

158. Pursuant to ORS 646A.602, "breach of the security" means "an unauthorized acquisition of computerized data that materially compromises the security, confidentiality or integrity of personal information that a person maintains or possesses." The Data Breach is a breach of AHS's security system, through which unauthorized persons acquired access to patients' personal information, including full names, addresses, dates of birth, driver's license or state identification numbers, Social Security numbers, claims information, financial account numbers, medications information, lab results, and medical diagnosis/conditions information., all of which is included within the definition for "personal information" provided within ORS 646A.602.

159. ORS 646A.604 requires any person or business that that conducts business in Oregon and that owns or licenses data that includes personal information to disclose any breach of

the security of its data system to any resident of the state whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person and the personal information was not secured. ORS 646A.604.

160. The statute further requires any person or business that maintains or possesses data that may include personal information that the person or business does not own or license to notify the owner or licensee of the information of any breach of the security of its data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person. ORS 646A.604.

161. Businesses must also provide the required notice to affected consumers "in the most expedient time possible, without unreasonable delay, and no more than forty-five calendar days after the breach was discovered." ORS 646A.604.

162. AHS's notice provided to the Plaintiff, does not state when AHS learned of the Data Breach. Rather, AHS stated the breach ended on March 17, 2022, and that it subsequently launched an investigation that concluded May 18, 2022. The Data Breach resulted in unauthorized access to the personal information, including PHI and PII, of hundreds of thousands of Oregon consumers.

163. In violation of this statute, AHS did not notify affected consumers about the Data Breach until July 13, 2022, approximately four months after it became aware of the breach. Furthermore, AHS waited another 55 days after its "investigation" concluded to notify affected consumers. This is clearly outside of the forty-five days articulated by the Oregon Consumer Information Protection Law and is certainly not "in the most expedient time possible."

164. AHS's willful and reckless violation of the provisions of this statute caused Plaintiff and the Class injury. AHS's delay allowed the hackers extended, unfettered access to Plaintiff's and the Class's PII and PHI for nefarious purposes.

165. Plaintiff and the Oregon Subclass were injured by AHS's violation of CIPA. Plaintiff and the Oregon Subclass seek all monetary and non-monetary relief allowed by law, including actual damages or statutory damages of $200 (whichever is greater), punitive damages, attorneys' fees and costs, and any additional relief this Court deems necessary or proper.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf all others similarly situated requests that the Court:

A. Certify this case as a class action on behalf of the Classes defined above, appoint Plaintiff, Lynda Kinne, as Class representative, and appoint the undersigned as Class counsel;

B. Award declaratory and other equitable relief as is necessary to protect the interests of Plaintiff and the Classes;

C. Award injunctive relief as is necessary to protect the interests of Plaintiff and the Classes;

D. Enter an award in favor of Plaintiff and the Classes that includes compensatory damages, including pre- and post-judgment interest thereon, in an amount to be proven at trial;

E. Award restitution and damages to Plaintiff and the Classes in an amount to be determined at trial;

F. Enter an award of attorneys' fees and costs, as allowed by law;

G. Grant Plaintiff and the Classes leave to amend this Complaint to conform to the evidence produced at trial; and

H. Grant such other or further relief as may be appropriate under the circumstances.

JURY DEMAND

Plaintiff hereby demands a trial by jury on all issues so triable.

Dated: September 15, 2022.

/s/ Bonner C. Walsh

Bonner C. Walsh (OSB 131716)
WALSH LLC
1561 Long Haul Road
Grangeville, ID 83530
Tel: (541) 359-2827
bonner@walshpllc.com

Christopher D. Jennings*
Nathan I. Reiter III*
THE JOHNSON FIRM
610 President Clinton Ave., Suite 300
Little Rock, AR 72201
Tel: (501) 372-1300
chris@yourattorney.com
nathan@yourattorney.com

Brian C. Gudmundson*
Jason P. Johnston*
ZIMMERMAN REED
1100 IDS Center, 80 South 8th Street
Minneapolis, MN 55402
Tel: (612) 341-0400
jason.johnston@zimmreed.com
brian.gudmundson@zimmreed.com

*To be admitted *pro hac vice*

Counsel for Plaintiff and the Proposed Class